AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* One (1) Google Account which information is stored at premises owned, maintained, controlled, or operated by Google LLC.	)	Case No. MJ24-092

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

One (1) Google Account which information is stored at premises owned, maintained, controlled, or operated by Google LLC.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2422(b)	Enticement of Children and Attempted Enticement of Children

The application is based on these facts:

✓ See Affidavit of Special Agent Alaina Dussler, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Alaina Dussler, Special Agent (HSI)

Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or

⊙ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 02/16/2024

Judge's signature

City and state: Seattle, Washington

S. Kate Vaughan, United States Magistrate Judge

Printed name and title

USAO: 2023R01224

AFFIDAVIT OF SPECIAL AGENT ALAINA DUSSLER

STATE OF WASHINGTON)
) ss
COUNTY OF SNOHOMISH)

I, Alaina Dussler, a Special Agent with Homeland Security Investigations, having been duly sworn, state as follows:

AFFIANT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Google accounts that are stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account.

2. I am a Special Agent ("SA") with the Department of Homeland Security ("DHS"), U.S. Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"). I have held such a position since December 2021. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States. I am currently assigned to the Office of the Special Agent in Charge ("SAC"), Seattle, Washington, and am a member of the Child Exploitation Investigations Group. As part of my current duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2252A. I have also had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)).

3. As part of my current duties as an HSI Criminal Investigator, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code, Sections 2251(a), 2252(a)(2), 2252(a)(4)(B), and 2243(a)(1). I have received training about child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography in various forms of media, including media stored on digital media storage devices such as computers, tablets, cellphones, etc. I am a graduate of the Criminal Investigator Training Program ("CITP"), and the HSI Special Agent Training ("HSISAT") at the Federal Law Enforcement Training Center in Glynco, Georgia. I have participated in the execution of previous search warrants, which involved child exploitation and/or child pornography offenses, and the search and seizure of computers, related peripherals, and computer media equipment. I am a member of the Seattle Internet Crimes Against Children Task Force ("ICAC"), and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code Section 2252A(a)(2), Distribution of Child Pornography, has been committed by BENNETT S. PARK resulting in Receipt of Child Pornography by the user of Google Account **jolenegauvreau98@gmail.com** (MV22 ACCOUNT). There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

INTRODUCTION AND PURPOSE OF AFFIDAVIT

6. I make this affidavit in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for location and account information associated with the Google account. The information is described in Attachment A, and is stored at premises controlled by Google LLC, a technology company headquartered at 1600 Amphitheatre Parkway, Mountain View, California. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 United States Code Section 2252A(a)(2), Distribution of Child Pornography has been committed by BENNETT S. PARK resulting in Receipt of Child Pornography by the user of Google Account **jolenegauvreau98@gmail.com** (MV22 ACCOUNT). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes further described in Attachment B.

7. This Court has jurisdiction to issue this requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated pursuant to 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

The following definitions apply to this affidavit:

8. "Chat," as used herein, refers to any kind of text communication over the internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as internet forums and email.

9. For the purposes of this affidavit, a "minor" refers to any person less than eighteen years of age and for the purpose of this search warrant, "Child pornography," as

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

10. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

11. "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that collectors of depictions of minors engaged in sexually explicit conduct can use to store and trade depictions of minors engaged in sexually explicit conduct in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders or collectors of depictions of minors engaged in sexually explicit conduct in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

12. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

related to or operating in conjunction with such device," including smartphones and mobile devices.

13. "Data," as used herein refers to the quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

14. "Digital Devices" as used herein refers to any physical object that has a computer, microcomputer, or hardware that is capable of receiving, storing, possessing, or potentially sending data.

15. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

16. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations, community-owned, non-profit, or otherwise privately-owned companies that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

17. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

18. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

19. "User Attributes," as used herein refers to any tangible data, documents, settings, programs, or other information that provides information related to the identity of the specific user of the device, computer, application, program, or record.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

BACKGROUND

Based on my training, experience and collaboration with agents/detectives investigation child exploitation, industry experts, academia and other law enforcement personnel, I know the following:

20. That adult persons with a sexual interest in minors are persons whose sexual targets are children. They receive sexual gratification and satisfaction from actual physical contact with children, fantasy involving the use of writings detailing physical contact with children, and/or from fantasy involving the use of pictures and/or videos of minors.

21. The development of the computer has changed the way children are engaged in sexually explicit conduct and the files created therefrom are distributed thereafter. The computer serves four functions in connection with depictions of children engaged in sexually explicit conduct. These four functions include: production, communications, distribution, and storage.

22. Pornographers produce both still and moving images, i.e.: photographs and video. These files can be transferred either directly from the camera/camera phone into a computer or mobile application, directly from a storage device such as a flash drive to a computer, or the image files can be transferred directly into the computer by use of a scanner.

23. In addition to data sharing between phones, mobile and desktop applications, and websites, e-mail may also be used electronically transmits files through a user's electronic device.

24. All that a smart phone or computer user needs to do in order to use an application, website, or email is open up an account with one of the myriad of companies that provide services (e.g. Meta, Microsoft, Google, Discord, Snapchat, Dropbox, etc.). Once the account is set up, the user can choose the "name" of his/her account, which does not have to match (or even relate to) identifying information of the user. Thus, the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

username by itself does nothing to identify the owner of the account, the user, or the composer of the communication. Nevertheless, often times the communications themselves, contain information that either directly or indirectly identifies the composer of the file. Based on my training and experience investigating child exploitation offenses, I know it is common for collectors of depictions of minors engaged in sexually explicit conduct to use multiple social media accounts and/or applications in order conceal their true identity and/or more easily categorize their collection according to the type of material or source.

25. Individuals involved in computer-related crimes often use these accounts to conduct both criminal and non-criminal communications. Consequently, these communications can be a great source of information to help identify the sender and/or recipient of the file and/or message. The ability to view these communications by investigating law enforcement often provides further investigative leads to assist in identifying the person of interest.

26. I know that an Internet Protocol (IP) address is a numerical label assigned to devices communicating on the internet and that the Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally. An IP address provides the methodology for communication between devices on the internet. It is a number that uniquely identifies a device on a computer network and, using transport protocols, moves information on the internet. Every device directly connected to the internet must have a unique IP address.

27. An IP address is typically comprised of four (4) series of numbers separated by periods and is most commonly represented as a 32-bit number such as 71.227.252.216 (Internet Protocol Version 4). IPv6 is deployed as well and is represented as a 128-bit number such as 2001:db8:0:1234:0:567:8:1.

28. IP addresses are owned by the Internet Service Provider and leased to a subscriber/customer for a period of time. They are public and visible to others as you

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

surf the internet. The lessee has no expectation of privacy due to the public nature of IP addresses.

29. When an Internet Service Provider's customer logs onto the internet using a computer or another web-enabled device, they are assigned an Internet Protocol (IP) address.

30. There are two different types of Internet Protocol addresses. The first is a dynamic IP address, which means the user's IP address may change each time they log on to the internet. The frequency in which this address changes is generally controlled by the Internet Service Provider and not the user. The other type of IP address is a static IP address, which means that a user is assigned a specific IP address that remains constant every time they log on to the internet.

31. IP addresses are similar to a license plate on a motor vehicle. They are the property of the issuer, and not the vehicle owner. Just as your license plate is visible as you cruise your city or town, your IP address is visible as you cruise the internet. Your IP address is visible to the administrators of websites you visit, attached emails you send, and broadcast during most internet file and information exchanges that occur on the internet.

32. I know based on my training and experience, that Electronic Service Providers ("ESP") and/or Internet Service Providers ("ISP," collectively ISP) typically monitor their services utilized by subscribers. To prevent their communication networks from serving as conduits for illicit activity and pursuant to the terms of user agreements, ISPs routinely and systematically attempt to identify suspected depictions of minors engaged in sexually explicit conduct that may be sent through its facilities. Commonly, customer complaints alert them that an image or video file being transmitted through their facilities likely contains suspected depictions of minors engaged in sexually explicit conduct.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

33. When an ESP/ISP receives such a complaint or other notice of suspected depictions of minors engaged in sexually explicit conduct, they may employ a "graphic review analyst" or an equivalent employee to open and look at the image or video file to form an opinion as to whether what is depicted likely meets the federal criminal definition of depictions of minors engaged in sexually explicit conduct found in 18 USC § 2256, which is defined as any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. If the employee concludes that the file contains what appears to be depictions of minors engaged in sexually explicit conduct, a hash value of the file can be generated by operation of a mathematical algorithm. A hash value is an alphanumeric sequence that is unique to a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, results in a different hash value. Consequently, an unknown image can be determined to be identical to an original file if it has the same hash value as the original. The hash value is, in essence, the unique fingerprint of that file, and when a match of the "fingerprint" occurs, the file also matches. Several different algorithms are commonly used to hash-identify files, including Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1).

34. Hash values are a very reliable method of authenticating files. It can be concluded with an extremely high degree of certainty that two files sharing the same hash value also share identical content. Based on my training and experience, as well as others

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

in this field, I know it is more likely that two humans would share the same biological DNA than for two files to share the same hash value. If even one bit (the smallest measure of data in a file) of a file is changed, the entire hash value of that file changes completely. As an example that demonstrates the uniqueness of a SHA-1 hash, the likelihood of two files having the same SHA-1 hash value is 2^{128} or:1 in 340,000,000,000,000,000,000,000,000,000,000,000,000 chance. In an August 6th, 2020 article in Live Science[1], according to Professor Simona Francese, PhD, a forensic scientist and fingerprint expert from Sheffield Hallam University in the United Kingdom, the likelihood of two humans having the same fingerprint is estimated to be:1 in 64,000,000,000.[2]

35. For two different files to have the same hash value is called a *collision.* I know from experience that there have been no documented incidents of a collision involving SHA-1 hash values "in the wild" since its creation in 1995. I am, however, aware of a reported collision involving two files sharing the same SHA-1 value in a lab setting. This was done purposely by engineers at Google[3] in 2017 under controlled conditions for the sole purpose of creating this collision. Even with this knowledge in mind, I am confident that the possibility of a suspected child sexual abuse material file reported in a CyberTip having the same hash value as an unrelated, non-criminal file is extremely unlikely. I believe hash value comparison is a highly reliable method of determining if two files are the same or different, and that a confirmed hash match between two files is a forensic finding on a par with a DNA match or a fingerprint match.

36. ESPs typically maintain a database of hash values of files that they have determined to meet the federal definition of depictions of minors engaged in sexually

---

[1] Baker, Harry. "Do Identical Twins Have Identical Fingerprints?" LiveScience, Purch, 7 Aug. 2021, https://www.livescience.com/do-identical-twins-have-identical-fingerprints.html.

[2] Of note, in the same article, Professor Francese, who is a peer-reviewed, published scientist, commented, "to this day, no two fingerprints have been found to be identical."

[3] "Announcing the First sha1 Collision." *Google Online Security Blog*, 23 Feb. 2017, https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

explicit conduct found in 18 USC § 2256. The ISPs typically do not maintain the actual suspect files themselves; once a file is determined to contain suspected depictions of minors engaged in sexually explicit conduct, the file is deleted from their system.

37. The ESPs can then use Image Detection and Filtering Process ("IDFP"), Photo DNA (pDNA), or a similar technology which compares the hash values of files embedded in or attached to transmitted files against their database containing what is essentially a catalog of hash values of files that have previously been identified as containing suspected depictions of minors engaged in sexually explicit conduct.

38. When the ESP detects a file passing through its network that has the same hash value as an image or video file of suspected depictions of minors engaged in sexually explicit conduct contained in the database through a variety of methods, the ISP reports that fact to National Center for Missing and Exploited Children (NCMEC) via the latter's CyberTipline. By statute, an ESP or ISP has a duty to report to NCMEC any apparent depictions of minors engaged in sexually explicit conduct it discovers "as soon as reasonably possible." 18 U.S.C. § 2258A(a)(1). The CyberTip line report transmits the intercepted file to NCMEC. Often that occurs without an ISP employee opening or viewing the file because the files hash value, or "fingerprint," has already been associated to a file of suspected depictions of minors engaged in sexually explicit conduct. The ISP's decision to report a file to NCMEC is made solely on the basis of the match of the unique hash value of the suspected depictions of minors engaged in sexually explicit conduct to the identical hash value in the suspect transmission.

39. ESP's also monitor which devices are used to access their platform by recording the advertising identification number. This number is a unique identifier assigned to hardware devices used by ESP's to track users semi-anonymously and provide targeted advertisements. Because it is a unique identifier, this information can link specific devices owned by specific individuals with the criminal activity on a particular platform's account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

40. Most Internet Service Providers keep subscriber records relating to the IP address they assign, and that information is available to investigators. Typically, an investigator has to submit legal process (e.g. subpoena or search warrant) requesting the subscriber information relating to a particular IP address at a specific date and time.

41. A variety of publicly available websites provide a public query/response protocol that is widely used for querying databases in order to determine the registrant or assignee of internet resources, such as a domain name or an IP address block. These include WHOIS, MaxMind, arin.net, and other common search tools.

42. The act of "downloading" is commonly described in computer networks as a means to receive data to a local system from a remote system, or to initiate such a data transfer. Examples of a remote system from which a download might be performed include a webserver, FTP server, email server, or other similar systems. A download can mean either any file that is offered for downloading or that has been downloaded, or the process of receiving such a file. The inverse operation, "uploading," refers to the sending of data from a local system to a remote system such as a server or another client with the intent that the remote system should store a copy of the data being transferred, or the initiation of such a process.

43. The National Center for Missing and Exploited Children (NCMEC) is a private, non-profit organization established in 1984 by the United States Congress. Primarily funded by the Justice Department, the NCMEC acts as an information clearinghouse and resource for parents, children, law enforcement agencies, schools, and communities to assist in locating missing children and to raise public awareness about ways to prevent child abduction, child sexual abuse and depictions of minors engaged in sexually explicit conduct.

44. The Center provides information to help locate children reported missing (by parental abduction, child abduction, or running away from home) and to assist physically and sexually abused children. In this resource capacity, the NCMEC

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

distributes photographs of missing children and accepts tips and information from the public. It also coordinates these activities with numerous state and federal law enforcement agencies.

45. The CyberTipline offers a means of reporting incidents of child sexual exploitation including the possession, manufacture, and/or distribution of depictions of minors engaged in sexually explicit conduct; online enticement; child prostitution; child sex tourism; extra familial child sexual molestation; unsolicited obscene material sent to a child; and misleading domain names, words, or digital images.

46. Any incidents reported to the CyberTipline online or by telephone go through this three-step process: CyberTipline operators review and prioritize each lead; NCMEC's Exploited Children Division analyzes tips and conducts additional research; The information is accessible to the FBI, ICE, and the USPIS via a secure Web connection. Information is also forwarded to the ICACs and pertinent international, state, and local authorities and, when appropriate, to the ESP.

47. Based upon my knowledge, experience, and training in depictions of minors engaged in sexually explicit conduct investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in depictions of minors engaged in sexually explicit conduct:

a. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years.

d. Likewise, those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

e. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other depictions of minors engaged in sexually explicit conduct distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contact and who share the same interests in depictions of minors engaged in sexually explicit conduct.

f. Those that possess, receive and attempt to receive depictions of minors engaged in sexually explicit conduct prefer not to be without their depictions of minors engaged in sexually explicit conduct for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of depictions of minors engaged in sexually explicit conduct throughout the world.

48. Based on my training and experience, collectors and distributors of depictions of minors engaged in sexually explicit conduct also use online, remote, resources to retrieve and store depictions of minors engaged in sexually explicit conduct, including services offered by many companies for cloud-storage and digital communications. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of electronic files in any variety of formats. A user can set up, and access, an online storage account from any computer or digital device with access to the internet. Evidence of such online storage of depictions of minors engaged in sexually explicit conduct is often found on the user's computer or smart phone. Even in cases where online storage is used, however, evidence of depictions of minors engaged in sexually explicit conduct can be found on a user's digital device if that device is used to access the internet. Cloud storage allows the offender ready access to the material from any device that has an internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device. Evidence located in cloud storage may be deleted from any device capable of reaching the website of the cloud hosting company. Once the individual user credentials, often a username and password are entered, the data in the cloud storage may be accessed, modified, shared, or deleted. Unlike deleting data from a local hard drive, once data is deleted from cloud storage, it is wiped from the cloud hosting company's servers and is unrecoverable.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

49. In addition to the traditional collector, law enforcement has encountered offenders who obtain depictions of minors engaged in sexually explicit conduct from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification.

50. Additionally, offenders may opt to store the contraband in cloud accounts. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage can span multiple servers, and often locations, and the physical environment is typically owned and managed by a hosting company. Cloud storage allows the offender ready access to the material from any device that has an internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device.

51. Based on my training and experience and my consultation with computer forensic detectives and agents who are familiar with searches of computers and smartphones, I have learned that offenders will try and obfuscate data containing images and videos of minors engaged in sexual activity. One potential manner of trying to hide the contraband may be by changing file extensions. For example, an image file may often have a file extension of ".jpg" of ".jpeg" signifying that it is an image or photograph. An offender may change the file extension by selecting the "save as" format on a computer or digital device and select ".doc" or ".docx" to make it appear that instead of a contraband image or photograph, it is a word document. The same process may be used to attempt to hide a video file as well. Based on these, and other attempts to hide potential

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contraband is necessary for forensic examiners to examine all potential data on a digital device.

52. I know that, regardless of whether a person discards or collects depictions of minors engaged in sexually explicit conduct he accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of depictions of minors engaged in sexually explicit conduct, backup files, and other electronic artifacts that may be forensically recoverable.

GOOGLE

53. Google is an online search engine, content platform, service provider, and information amalgamator. Since their debut Google currently maintains a variety of online content products and services and they are ranked as one of the most frequently visited web sites in the United States. The following information was gleaned from Google's website, privacy policy and other on-line resources. Google offers a large number of products including Gmail, Chrome Web Browser, Waze, YouTube, Chromecast, Google Home, Android, Google Auto, Google Maps, Gmail, the Google+ social media site, photo hosting platforms and many others. In addition to information Google obtains from a user using their services, Google collects data on a user from other companies doing business on the internet. They amalgamate the data in order to sell advertising aimed at the specific user.

54. Google identifies accounts in a variety of ways, primarily by Gmail account, but also telephone number, or IMEI number of an Android device. Basic data that Google stores about users include:

- Name, gender, and date of birth
- Email addresses

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

- Phone numbers
- Websites visited
- Searches made on Google Search
- Ad preferences
- YouTube search history and recently watched videos

55. Location data is also collected and stored by Google. They use advanced location recognition technology in order to routinely calculate your location. Android phones, which run off of Google's services, and Pixel, Google's own phone, track and record a user's location through several means, including Wi-Fi, GPS, and cellular networks. Other more specific types of information collected and stored by Google include the following:

a. Account Information - User name, primary email address, secondary email addresses, connected applications and sites, and account activity, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;

b. Android Information - Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device;

c. Evidence of user attribution - accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).

d. Calendar - Calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. Contacts - Contacts stored by Google including name, contact phone numbers, emails, social network links, and images;

f. Documents – All user created documents stored by Google;

g. Finance - Records of securities, funds, and portfolios associated with the target Google account and/or target device;

h. Gmail - All email messages, including inbox messages, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages include information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and attached files;

i. Google Photos - Images, graphic files, video files, and other media files stored in the Google Photos service;

j. Location History - Location data including that derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data typically includes the GPS coordinates and the dates and times of all location recordings;

k. Play Store - Applications downloaded, installed, and/or purchased by the associated account and/or device;

l. Search History - All search history and queries;

m. Voice - Call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device;

n. Google Home – Information related to Google Home including, but not limited to, device names, serial numbers, Wi-Fi networks, addresses, media services,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

linked devices, video services, voice and audio activity, and voice recordings with dates and times.

o. Google Assistant – Information related to Google Assistant including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings with dates and times.

p. Android Auto – Information related to Android Auto including, but not limited to, device names, serial numbers and identification numbers, device names, maps and map data, communications including call logs and text messages, voice actions, and location data.

q. Android Drive – Data stored in the Google Drive for the listed account.

SUMMARY OF PROBABLE CAUSE

CR23-191 United States v. Bennett S. Park – Production of Child Pornography

56. Homeland Security Investigations (HSI) identified Bennett S. Park age 42 during an undercover operation that took place in King County on July 7, 2023. Park responded to an online platform advertisement that read "single mom with 2lils bored @ home" by informing the undercover ad poster that he was sexually attracted to young girls and was interested in meeting the undercover's 7- and 10-year-old daughters. Park claimed he had previously been sexually active with children ranging from age 11-17 years old. Park described the sexual things he wished to do to the undercover's children. The undercover continued chatting with Park through August 2023.

57. On August 8, 2023, Park informed the undercover he was going to pick up a 13-year-old female with whom he was chatting online, engage in sexual activity with the child, and film the abuse. HSI immediately surveilled Park's Snohomish County residence, followed him to a location in Everett at 1:45 a.m., observed a 13-year-old female enter his car, intervened, and placed Park under arrest. A subsequent search

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

warrant return from the platform Discord documented Park's communications with the 13-year-old female to include his knowledge of her age and intention to sexually abuse her. Sexual Assault charges against Park are pending in Snohomish County.

58. A residential search warrant was executed on Park's home in August 2023 and resulted in the seizure of several devices which are in various stages of forensic examination. Subsequent search warrants to online platforms have confirmed Park's prolific use of social media applications to sexually exploit minors following a slew of Cybertips relating to Park's online child exploitation. 23 apparent minors have been identified thus far ranging from ages 10 through 17.

59. In October 2023, HSI agents located chats between Park and a 12-year-old female in which Park acknowledged her age, repeatedly asked for sexually imagery of the child, repeatedly and graphically discussed the sexual activity he wished to engage in with the minor, and his receipt of numerous files of the child engaging in acts of self-exploitation. As a result, Park was indicted on one count of Production of Child Pornography in violation of Title 18, United States Code, Sections 2251(a), 2251(e) in the Western District of Washington on December 13, 2023, and is pending trial.

Park's Google Cybertip 171040890 Involving Minor Victim 22

60. On or about August 17, 2023, HSI Seattle received a CyberTip from via the National Center for Missing and Exploited Children (NCMEC) under CyberTip number 171040890. CyberTip 171040890 reported eight message threads between the reported account and minor children. The reported message threads dates span from approximately 2019 to 2022 and the reported conversations appear to be predominantly sexual in nature and/or appear to show the reported account engaging in grooming behaviors with the minor child accounts. The reported account is listed below as follows and will be referred to as DISCORD 2.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

DISCORD 2

Phone: 510-717-9227

Email Address: bennettspark@gmail.com

Username: MoonMan#4642

User ID: 432783654557843456

Related CyberTips: 171040890, 52961381

61. In one particular message thread between DISCORD 2 and a minor child account that will be referenced as MV22, it appears that DISCORD 2 may have emailed CSAM to the MV22 ACCOUNT on or about June 30, 2019. The Discord chats began around May 25, 2019, at approximately 20:32:19 UTC. The following are excerpts from the messages between DISCORD 2 and MV22.

[Timestamp 05/25/2019 20:32:19 UTC]

DISCORD 2: Hi

DISCORD 2: I think i added you off kidschat

MV22: Oh okay hi

MV22: What was your kc username?

DISCORD 2: It was TheFade. I'm not on there much though.

MV22: Ohhh okay

MV22: never heard of it tho lmao

DISCORD 2: Lol ya do you go on there a lot?

MV22: Yeah

[Timestamp 05/25/2019 20:41:49 UTC]

[…]

[Timestamp 05/25/2019 20:44:18 UTC]

MV22: but my Nickname is Fish

DISCORD 2: What's your asl? If you don't mind.

DISCORD 2: Lol cute. Do you swim a lot of something

MV22: I'm 12, F, canada

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

DISCORD 2: Oof, ok (:

MV22: naw idk how it started. i missed a day of school and everyone just started calling me Fish oof

DISCORD 2: Lol wonder why. It's cute though

MV22: Lmao thanks

DISCORD 2: Yw which part of Canada are you in?

MV22: Saskatchewan

MV22: used to live in BC about 4 years ago, but we moved unfortunately

DISCORD 2: Aw I see. I live right below BC in Seattle

DISCORD 2: So I visit Vancouver sometimes

MV22: Oh okay, I used to live in Victoria

DISCORD 2: Oh coool. It's pretty there.

MV22: Yeah. too many pretentious people there ngl

DISCORD 2: What does ngl mean?

MV22: Not gonna lie

DISCORD 2: Ah of course. Sorry I'm kinda older so idk some stuff like that haha

MV22: Oh lol it's fine

MV22: may i ask what your age is?

DISCORD 2: lol thanks. Gah I don't wanna scare you away cuz you seem nice.

DISCORD 2: Cuz im considerably older…

MV22: Oh okay no problem

MV22: but under 19 considering you are still on kc right?

DISCORD 2: No I'm older ><

DISCORD 2: People tell me I look you g for my age

MV22: Oh oof

DISCORD 2: Tbh seems like there's lots of older guys who go on kc

MV22: yeah ik

MV22: honestly most are just pedophiles

MV22: especially the guests

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

DISCORD 2: Yeah I figured

DISCORD 2: To be really honest im basically one too… that's why I was on there

MV22: Uh

DISCORD 2: I'm not like the idiots that you've seen on kc though

MV22: What do you mean by that?

MV22: like

MV22: idiotic in which way

DISCORD 2: I mean like blatantly perverted

DISCORD 2: I date women my age too but I'm also attracted to younger girls, that's all I'm saying

MV22: Oh uh okay

DISCORD 2: Lol sorry for creeping you out. Just being honest

MV22: It's fine

DISCORD 2: Thanks. So what does Fusg mean?

MV22: One of my friends made a typo when typing "fish" and it was "fusg"

DISCORD 2: Oh hahaha

MV22: so everyone made fun of her and started calling me "fusg" XD

[Timestamp 05/25/2019 22:42:45 UTC]

[…]

[Timestamp 05/25/2019 22:44:46 UTC]

DISCORD 2: Is she 12 too

MV22: no she's 13

DISCORD 2: May I see a pic of you? ><

MV22: I actually had to reset my computer a few days ago so i don't have any pictures of me. Unfortunately all my other stuff was gone too

DISCORD 2: Boooo

MV22: Yeah ikr

[Timestamp 05/25/2019 22:57:17 UTC]

[Timestamp 06/30/2019 07:17:40 UTC]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

DISCORD 2: Lol great username

MV22: Lmao thanks

DISCORD 2: Yw (: so why are you up now young lady

MV22: Eh I usually stay up

DISCORD 2: Same. I forgot you're 12 right

MV22: Yeah

DISCORD 2: Isn't that a little young to be naming yourself emo whore haha

MV22: Nah lmao

DISCORD 2: Lol ya ok. I guess not.

MV22: Yep

DISCORD 2: Hm are you really a whore though lol

MV22: Uh people def see me as one

DISCORD 2: Really why

MV22: I don't know

DISCORD 2: Do you dress a certain way

MV22: Nope

DISCORD 2: I bet you look nice in a skirt (:

MV22: Oof

MV22: Thanks

DISCORD 2: Yw. And socks too

MV22: yeah maybe

DISCORD 2: Do you like knee high and thigh high socks!

MV22: Uh I guess

DISCORD 2: Do you have any skirts you like

MV22: Nope

MV22: I don't usually wear skirts

DISCORD 2: I'm going to make you wear a skirt one day

MV22: Lmao okay

DISCORD 2: And imma take pics too

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

MV22: Ooof

MV22: Wait

MV22: how old are you again?

DISCORD 2: Lol well I'm older…

MV22: Like.. how old

DISCORD 2: I don't wanna like scare you away

MV22: I talked to older guys before lmao, I'm not scared

MV22: I won't block you or anything

DISCORD 2: Cool (: well I'm over 30…

MV22: Ooof okay

DISCORD 2: People think I'm younger all the time but yea oof

MV22: Why did you go on kidschat when you only associate with dumb 13 year-olds?

DISCORD 2: Lol I don't go on there a lot

MV22: Oh okay

DISCORD 2: I'll be completely honest I'm attracted to girls that age

MV22: Oh okay oof

DISCORD 2: I'm kinduva lolicon

MV22: Wait what's that again?

DISCORD 2: An older man who likes young girls basically p

MV22: Oh mmk

DISCORD 2: Tbh I've met and done things with girls your age

MV22: Damn oof

DISCORD 2: Yeah ikr… I've taken pics and vids of it too…

MV22: Damn..

MV22: Why though?

DISCORD 2: Tbh I get off on it and jerk off to them later

MV22: Oooofff

MV22: Have you like.. ever got caught?

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

DISCORD 2: No I haven't

DISCORD 2: Otherwise I wouldn't be here to chat with you rn haha

MV22: Yeah true hah

DISCORD 2: And tbh I know the girls all liked it cuz they want more and they keep it a secret

MV22: Oof.. they did?

DISCORD 2: Yes

DISCORD 2: I could even show you pics, but… ya

MV22: Lmao I dare you

MV22: prove itttt

DISCORD 2: Lol hmmm not on here

DISCORD 2: I'll get banned if I share those with you on here

MV22: Oh okay

MV22: wait

MV22: you can get banned on disc?

DISCORD 2: Idk honestly but I heard if you share illegal stuff you can get banned p

MV22: Well one of my friends has and he didn't get banned :P

DISCORD 2: Oof What did he share

MV22: He shared ass pics as a joke

DISCORD 2: Oh ok

MV22: another one of my friends sent tit pics as a joke and she didn't get caught

DISCORD 2: Those aren't illegal though

DISCORD 2: And btw your bf bean is texting me

MV22: she's underage

MV22: But yeah oof he's overprotective

DISCORD 2: Ohhh

DISCORD 2: You didn't need to screenshot my messages to him sheesh

MV22: I didn't screenshot them lmao

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

MV22: I just told him about it

DISCORD 2: Hmm ok well he added me

MV22: Oof okay

DISCORD 2: And yeah I'm not showing you those pics

MV22: anyway

MV22: Fair enough lmao

MV22: But how would I believe it?

DISCORD 2: Believe what

MV22: That you actually did those things

DISCORD 2: It's all a lie I made up

MV22: hmm

DISCORD 2: I would show you if you promised not to tell your jealous bf lol

MV22: I swear I won't lmao

MV22: I dont break promises

DISCORD 2: lol ya right

MV22: I promise lmao

MV22: I don't break promises

DISCORD 2: Do you have Snapchat

MV22: Nope

MV22: do you have hangouts?

DISCORD 2: Yeah…

MV22: Kk

MV22: what is it

DISCORD 2: Just tell me ur email and I'll email them to you

MV22: jolenegauvreau98@gmail.com

DISCORD 2: Ok it might take a while

MV22: Kk

DISCORD 2: Will you at least show me a pic of you

MV22: sure

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

MV22: just wait

DISCORD 2: I have to warn you these pics are really graphic/sexual

MV22: I guessed

MV22: [Sends image titled avatar_user1002605_7034720395039536.jpg. The image shows a female child's face with her chin resting on the child's left hand. The child appears to be wearing a purple shirt. Based on the child's youthful features, the child appears to be approximately 11-13 years old.]

MV22: that's me

DISCORD 2: Aw you look like an angel

MV22: Thanks XD

MV22: Did they send?

DISCORD 2: Sorry I'm having issues accessing them I'm still looking

MV22: Okey

DISCORD 2: May I see another pic of you

MV22: I don't have another one. I just started getting my stuff back on my computer

DISCORD 2: K I sent one…

DISCORD 2: Promise to be a good little girl and not show or tell anyone

MV22: I won't

MV22: I promise

DISCORD 2: Did you see the first one I sent

MV22: Yeah

MV22: You sent more?

DISCORD 2: I will

DISCORD 2: What did you think though

MV22: Uh idk, am I supposed to think something?

DISCORD 2: Lol no

DISCORD 2: Do you want to see more though

MV22: Yeah

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

DISCORD 2: Did you like the first pic

MV22: mhm

DISCORD 2: Good (:

DISCORD 2: I could even show you videos but idk…

MV22: Sure

DISCORD 2: I sent another one…

DISCORD 2: Can you guess what's on her panties

MV22: Obviously cum lmao

DISCORD 2: Lol they were cute panties

MV22: yeah

DISCORD 2: Would you let me cum on your panties like that lol

MV22: Idk

DISCORD 2: Did you like that pic too

MV22: Yeah

MV22: first one was better tho

DISCORD 2: I could show you more but she's really young…

MV22: weren't the last ones already young? I don't think it matters tbh

DISCORD 2: Yeah true and thx

MV22: np

DISCORD 2: K I sent more

MV22: kk

DISCORD 2: So are you showing people

MV22: No

MV22: Why would I

DISCORD 2: Did you get the last set

MV22: Yeah

DISCORD 2: how old was she?

DISCORD 2: What would you guess

MV22: 8?

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

DISCORD 2: No 10 or 11

DISCORD 2: She was really petite

MV22: I noticed yeah

DISCORD 2: Did you like the pics though

MV22: Yeah

DISCORD 2: Do you still want to see more then

MV22: Definitely

DISCORD 2: Tbh I wish I could take pics with you

MV22: Oof okay

DISCORD 2: I really mean that especially after seeing your pic

MV22: yeah

DISCORD 2: Is there any part of you that would like that

MV22: I don't know

DISCORD 2: I sent a couple more

DISCORD 2: I had to edit the environment on one of them

MV22: Oh, why's that?

DISCORD 2: Eh to hide things

DISCORD 2: Do you see it

MV22: yeah

DISCORD 2: I liked her piglet socks (:

MV22: Yeah

DISCORD 2: I sent more

DISCORD 2: I met these girls off an app and they basically let me do anything to them…

MV22: Wow

DISCORD 2: Yeah… do you like it

MV22: I didn't open them yet

DISCORD 2: Let me know what you think of them

MV22: How ol were the girls?

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

MV22: old*

DISCORD 2: How old do you think

MV22: 13?

DISCORD 2: Yeah

MV22: oof

DISCORD 2: Do you like those pics

MV22: Yeah

DISCORD 2: Do you really mean that

MV22: Yeah

DISCORD 2: Btw what state do you live in

MV22: I live in Canada

DISCORD 2: Cool which part?

MV22: Sask.

DISCORD 2: Would be nice to visit you there and do this with you too (:

[Timestamp 06/30/2019 09:58:57 UTC]

62. CyberTip 171040890 noted that there was one other associated CyberTip to MV22's Discord account under CyberTip 52961381. On or about October 18, 2023, HSI Seattle received a copy of the associated CyberTip 52961381.

63. CyberTip 52961381 was originally reported on or about July 30, 2019, by Discord regarding MV22's Discord account sharing alleged CSAM files with another user. The CyberTip reported 6 CSAM files that had originally been uploaded by MV22's Discord on June 30, 2019, between 8:37:24 UTC and 18:40:52 UTC, which matches with the timeframe DISCORD 2 was apparently emailing CSAM to the MV22 ACCOUNT. An example of two of the reported files are as follows.

File Name: 1429322269051-0.jpg

MD5: 533bbba3c63805348e33adeecb86f4f8

Did ESP view File Contents? Yes

IP Address: 74.127.196.148

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Upload Time/Date: 06/30/2019 09:16:49 UTC

Description: The image shows a female child lying naked on her stomach on brown colored carpeting. The child is facing away from the camera with her head towards a light purple wall. The child is wearing black animal ears on a headband and her head is looking over her right shoulder to look at the camera. The child has her legs spread apart to expose her vagina. Based on the child's size, youthful features, lack of muscle and hip development and lack of pubic hair, it appears the child is approximately between 9-11 years old.[4]

File Name: 1423126575427-1.jpg

MD5: 4aa2f343b50332be92c5d8ba7f05532b

Did ESP view File Contents? Yes

IP Address: 74.127.198.254

Upload Time/Date: 06/30/2019 18:31:20 UTC

Description: The image shows a female child lying naked on her back with her legs bent at the knees and spread apart. The child is holding her buttocks to expose her vagina. The child appears to be lying on-top of an adult male, whose penis is vaginally penetrating the child. The adult male's face is not visible in the image and the space behind the child's head appears to be warped. Based on the child's size, muscle development, early breast development and early pubic hair development it appears the child is approximately 12-14 years old.[5]

64. On or about November 7, 2023, HSI Seattle issued a search warrant to Google for account contents relating to the email associated with DISCORD 2,

[4] I have viewed this file and based on my training and experience, I believe the file described above meets the federal definition of child pornography, as defined in 18 U.S.C. 2256(8).

[5] I have viewed this file and based on my training and experience, I believe the file described above meets the federal definition of child pornography, as defined in 18 U.S.C. 2256(8).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

bennettspark@gmail.com, however, no correspondence to or from the MV22 ACCOUNT was discovered in the results provided.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

65. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

66. As set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code Section 2252A(a)(2), Distribution of Child Pornography have been committed by BENNETT S. PARK resulting in the Receipt of Child Pornography by the user of Google Account **jolenegauvreau98@gmail.com** (MV22 ACCOUNT). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes further described in Attachment B.

Alaina Dussler, Affiant
Special Agent, HSI

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on this 16th day of February, 2024.

S. Kate Vaughan
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Google account **jolenegauvreau98@gmail.com** which information is stored at premises owned, maintained, controlled, or operated by Google LLC, a technology company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by Google LLC.

To the extent that the information described in Attachment A is within the possession, custody, or control of Google (the Provider), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Google, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for the user listed in Attachment A **jolenegauvreau98@gmail.com** the following data:

1. Subscriber's name and address;

2. Length of service including start date and time and initial log in IP address;

3. Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address, as well as all devices used to access the account, including IMEI numbers, ICCID numbers, and all descriptions of make and model, associated push tokens;

4. Subscriber's additional email account names, addresses and messenger aliases associated with the account above;

5. Records of communications between Google, and the accountholder, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications;

6. A list of the various types of services and activities data for of the above account including an index of MyDashboard listing the products being accessed by the user, including: the name of the Google account holder, the google email address of the account holder, searches run using the Google search engine by the account holder, a record of the types of devices used to access the Google account, Allo Google assistance,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Cloud Print, Google Books, Google Audio, Google Drive, Google conversations, Google Chrome, Google Chrome Sync, Google Photos, Google Groups, Calendar, Contacts, Keep, Location History, Maps (your places), My Maps, Google Voice, Google Wallet, Play Store, Profile, and YouTube;

7. Means and source of payment for such service (including any credit card or bank account number);

8. Information relating to the identity of the subscriber;

9. Devices associated with the Google account above, to include all advertising identification number(s);

10. Google Wallet payment information such as associated credit card numbers used to facilitate purchases and data such as the billing address of any linked credit card;

11. All images, photos, or videos, in whatever format, associated with or stored in the above account;

12. Messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified (user attribution data);

13. Logs/history of Internet Protocol to assist in identifying the suspect(s);

14. E-mails, including content, recipient(s), sender(s), and date and time stamp, sent and received during the above date range to establish dominion and control over the account;

15. Location or GPS data collected and stored by Google for the account to provide user attribution.

Google LLC is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 United States Code Section 2252A(a)(2), Distribution of Child Pornography by BENNETT S. PARK resulting in Receipt of Child Pornography by user

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

jolenegauvreau98@gmail.com as listed on Attachment A, information pertaining to the following matters between the dates of **May 25, 2019, and July 1, 2019**:

1. All child pornographic or child erotic photos, videos, and other files associated with the Account which are stored using the remote storage and synchronization service commonly known as Google Drive, or which have been deleted therefrom;

2. All child pornographic or child erotic photos and files associated with the Account in the image organizer and image viewer commonly known as Picasa and/or Google Picasa;

3. The contents of all emails and instant message communications associated with the Account, including stored or preserved copies of emails sent to and from the Account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

4. Any images, videos, emails, instant message communications, records, files, logs, current information, or information or images or videos that have been deleted but are still available to the Provider, or which have been preserved pursuant to a request to preserve the account;

5. All records or other information regarding the identification of the Account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the Account was created, devices associated with the account, the length of service, the IP address used to register the Account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

6. Any photos, documents, or other files that may indicate user attribution or ownership of the Account;

7. The types of service utilized or associated with the Account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

8. All records or other information stored at any time by an individual using the Account, including address books, contact and buddy lists, calendar data, pictures, and files;

9. All records pertaining to communications between the Provider and any person regarding the Account, including contacts with support services and records of actions taken;

10. All records and other information concerning any computer file created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

11. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored;

12. Evidence indicating how and when the Account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crimes under investigation and to the Account owner;

13. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

14. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970